

December 2020

**Test Results for Binary Image (JTAG, Chip-Off) Decoding and  
Analysis Tool: Oxygen Forensic Detective v13.1.0.43**

## Contents

Introduction.....	1
How to Read This Report .....	1
1 Results Summary .....	2
2 Mobile Device Binary Images .....	3
3 Testing Environment.....	3
3.1 Execution Environment .....	3
3.2 Internal Memory Data Objects.....	3
4 Test Results.....	5
4.1 Chip-Off Data Extractions .....	6
4.2 JTAG Data Extractions .....	9

## Introduction

The Computer Forensics Tool Testing (CFTT) program is a joint project of the Department of Homeland Security (DHS), the National Institute of Justice (NIJ), and the National Institute of Standards and Technology Special Program Office (SPO) and Information Technology Laboratory (ITL). CFTT is supported by other organizations, including the Federal Bureau of Investigation, the U.S. Department of Defense Cyber Crime Center, U.S. Internal Revenue Service Criminal Investigation Division Electronic Crimes Program, and DHS's Bureau of Immigration and Customs Enforcement, U.S. Customs and Border Protection and U.S. Secret Service. The objective of the CFTT program is to provide measurable assurance to practitioners, researchers, and other applicable users that the tools used in computer forensics investigations provide accurate results. Accomplishing this requires the development of specifications and test methods for computer forensics tools and subsequent testing of specific tools against those specifications.

Test results provide the information necessary for developers to improve tools, users to make informed choices, and the legal community and others to understand the tools' capabilities. The CFTT approach to testing computer forensics tools is based on well-recognized methodologies for conformance and quality testing. Interested parties in the computer forensics community can review and comment on the specifications and test methods posted on the CFTT Web site (<https://www.cftt.nist.gov/>).

This document reports the results from testing Oxygen Forensic Detective v13.1.0.43 decoding and analysis of mobile devices JTAG and chip-off binaries.

Test results from other tools can be found on the DHS S&T-sponsored digital forensics web page, <https://www.dhs.gov/science-and-technology/nist-cftt-reports>.

Thanks and appreciation to Rex Kiser and team from the Fort Worth Police Department – Digital Forensics Lab and Steve Watson and team from VTO Labs for their assistance on performing Chip-Off data extractions.

## How to Read This Report

This report is divided into four sections. Section 1 identifies and provides a summary of any significant anomalies observed in the test runs. This section is sufficient for most readers to assess the suitability of the tool for the intended use. Section 2 identifies the mobile devices used for testing. Section 3 lists testing environment, the internal memory data objects used to populate the mobile devices. Section 4 provides an overview of the test case results reported by the tool.

# Test Results for Binary Image (JTAG, Chip-Off) Decoding and Analysis Tool

Tool Tested: Forensic Detective v13.1.0.43

Software Version: v13.1.0.43

Supplier: Oxygen

Address: 909 N. Washington St, Suite 300  
Alexandria, VA 22314

Fax: +1(703) 888-2327

WWW: [oxygen-forensic.com](http://oxygen-forensic.com)

## 1 Results Summary

Forensic Detective v13.1.0.43 was tested for its ability to decode and analyze binary images created by performing Chip-Off and JTAG data extractions from supported mobile devices. Except for the following anomalies, the tool was able to decode and report all supported data objects completely and accurately for all mobile devices tested.

### ***SMS, MMS Data:***

- Incoming MMS messages were not reported. (Device: *LG K7\_Chip-off*)

### ***Browser Data:***

- Browser data was not reported. (Device: *LG K7\_Chip-off*)

### ***Social media Data:***

- Social media related data (i.e., Twitter) is partially reported. (Device: *LG K7\_Chip-off*)
- Social media related data (i.e., Facebook) is partially reported. (Devices: *HTC One XL\_Chip-off, HTC One XL\_JTAG*)

For more test result details see section 4.

## 2 Mobile Device Binary Images

The following table lists the mobile device binaries used for testing Forensic Detective v13.1.0.43.

Make	Model	OS Version	Data Extraction
HTC	Desire S	Android 2.3 Gingerbread	Chip-Off, JTAG
HTC	One Mini	Android 4.2 Jelly Bean	Chip-Off, JTAG
HTC	One XL	Android 4.0 Ice Cream Sandwich	Chip-Off, JTAG
Samsung	S4	Android 4.2 Jelly Bean	Chip-Off, JTAG
HTC	Desire 626	Android 5.1 Lollipop	Chip-Off
Motorola	Moto-E	Android 5.1 Lollipop	Chip-Off
LG	K7	Android 5.1 Lollipop	Chip-Off
ZTE	Z970	Android 4.4 KitKat	Chip-Off
Samsung	S2	Android v2.3 Gingerbread	Chip-Off

Table 1: Mobile Device Binary Images

## 3 Testing Environment

The tests were run in the NIST CFTT lab. This section describes the selected test execution environment, and the data objects populated onto the internal memory of mobile devices.

### 3.1 Execution Environment

Forensic Detective v13.1.0.43 was installed on Windows 10 Pro version 10.0.14393.

### 3.2 Internal Memory Data Objects

Forensic Detective v13.1.0.43 was measured by analyzing acquired data from the internal memory of pre-populated mobile devices. Table 2 defines the data objects and elements used for populating mobile devices provided the mobile device supports the data element.

Data Objects	Data Elements
Address Book Entries	<i>Regular Length</i>
	<i>Maximum Length</i>
	<i>Special Character</i>
	<i>Blank Name</i>
	<i>Regular Length, email</i>
	<i>Regular Length, graphic</i>
	<i>Regular Length, Address</i>
	<i>Deleted Entry</i>
	<i>Non-Latin Entry</i>
	<i>Contact Groups</i>

<b>Data Objects</b>	<b>Data Elements</b>
PIM Data: Datebook/Calendar; Memos	<i>Regular Length</i>
	<i>Maximum Length</i>
	<i>Deleted Entry</i>
	<i>Special Character</i>
	<i>Blank Entry</i>
Call Logs	<i>Incoming</i>
	<i>Outgoing</i>
	<i>Missed</i>
	<i>Incoming – Deleted</i>
	<i>Outgoing – Deleted</i>
	<i>Missed - Deleted</i>
Text Messages	<i>Incoming SMS – Read</i>
	<i>Incoming SMS – Unread</i>
	<i>Outgoing SMS</i>
	<i>Incoming EMS – Read</i>
	<i>Incoming EMS – Unread</i>
	<i>Outgoing EMS</i>
	<i>Incoming SMS – Deleted</i>
	<i>Outgoing SMS – Deleted</i>
	<i>Incoming EMS – Deleted</i>
	<i>Outgoing EMS – Deleted</i>
<i>Non-Latin SMS/EMS</i>	
MMS Messages	<i>Incoming Audio</i>
	<i>Incoming Graphic</i>
	<i>Incoming Video</i>
	<i>Outgoing Audio</i>
	<i>Outgoing Graphic</i>
	<i>Outgoing Video</i>
Application Data	<i>Device Specific App Data</i>
Stand-alone data files	<i>Audio</i>
	<i>Graphic</i>
	<i>Video</i>
	<i>Audio – Deleted</i>
	<i>Graphic - Deleted</i>
	<i>Video - Deleted</i>
Internet Data	<i>Visited Sites</i>
	<i>Bookmarks</i>
	<i>E-mail</i>
Location Data	<i>GPS Coordinates</i>
	<i>Geo-tagged Data</i>
Social Media Data	<i>Facebook</i>
	<i>Twitter</i>
	<i>LinkedIn</i>
	<i>Instagram</i>

Data Objects	Data Elements
	<i>Pinterest</i>
	<i>SnapChat</i>
	<i>WhatsApp</i>

**Table 2: Internal Memory Data Objects**

## 4 Test Results

This section provides the test case results reported by the tool. Sections 4.1 – 4.2 identify the make and model of the mobile device used for creating the binary image and data extraction technique employed i.e., Chip-Off, JTAG.

The *Test Cases* column in sections 4.1 and 4.2 are comprised of two sub-columns that define a particular test category and individual sub-categories that are verified when decoding and analyzing the associated binary image. The results are as follows:

*As Expected:* the mobile forensic application returned expected test results – the tool imported, analyzed and reported data from the mobile device image file successfully.

*Partial:* the mobile forensic application returned some of the data from the mobile device image file.

*Not As Expected:* the mobile forensic application failed to return expected test results – the tool did not report supported data from the mobile device image file successfully.

*NA:* Not Applicable – the mobile forensic application is unable to perform the test or the tool does not provide support for the acquisition of a particular data element.

## 4.1 Chip-Off Data Extractions

The internal memory contents for Chip-Off binary images were decoded and analyzed with Forensic Detective v13.1.0.43.

All test cases pertaining to the acquisition of supported Android devices were successful with the exception of the following.

- Incoming MMS messages (audio, graphic, video) were not reported for the LG K7.
- Browser related data (history, bookmarks) were not reported for the LG K7.
- Twitter social media data was partially reported i.e., account related information for the LG K7.
- Facebook social media data was partially reported i.e., account related information for the HTC One XL.

### Notes:

*-Devices defined in the table below with an ‘\*’ e.g., HTC One XL\*, both Chip-Off and JTAG data extractions were performed.*

- Deleted Contacts, Calendar, Memo/Note entries were recovered for the Samsung S4 and Samsung S2.
- Deleted Contacts and Calendar entries were recovered for the HTC Desire 626, Moto-E, LG K7, ZTE 970, HTC One XL, HTC Desire S and Moto-E.
- Deleted Contacts were recovered for the HTC One Mini.
- Deleted Call logs were recovered for the LG K7, ZTE 970, HTC One Mini, HTC Desire S and Samsung S2.
- Deleted SMS entries were recovered for the HTC Desire 626, ZTE 970, Samsung S2, HTC One XL, Samsung S4, HTC One Mini, HTC Desire S and Moto-E
- Deleted bookmark entries were recovered for the HTC Desire 626, Samsung S2, HTC One XL, HTC Desire S and Moto-E.

See Table 3 below for more details.



## Forensic Detective v13.1.0.43

Test Cases – Chip-Off Binary Decoding and Analysis		Mobile Device Binary Images: Chip-Off								
		HTC Desire 626	LG K7	ZTE 970	Samsung S2	HTC One XL*	Samsung S4*	HTC One Mini*	HTC Desire S*	Moto-E
Equipment/ User Data	IMEI	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	MEID/ESN	NA	NA	NA	NA	NA	NA	NA	NA	NA
	MSISDN	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
PIM Data	Contacts	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Calendar	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Memos/ Notes	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Call Logs	Incoming	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Outgoing	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Missed	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
SMS Messages	Incoming	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Outgoing	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
MMS Messages	Graphic	As <i>Expected</i>	Partial	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Audio	As <i>Expected</i>	Partial	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Video	As <i>Expected</i>	Partial	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Stand-alone Files	Graphic	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Audio	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Video	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Application Data	Documents (txt, pdf files)	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Social Media Data	Facebook	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	Partial	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Twitter	As <i>Expected</i>	Partial	NA	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	LinkedIn	As <i>Expected</i>	As <i>Expected</i>	NA	NA	NA	NA	NA	NA	As <i>Expected</i>
	Instagram	As <i>Expected</i>	As <i>Expected</i>	NA	As <i>Expected</i>	NA	As <i>Expected</i>	As <i>Expected</i>	NA	As <i>Expected</i>

## Forensic Detective v13.1.0.43

Test Cases – Chip-Off Binary Decoding and Analysis		Mobile Device Binary Images: Chip-Off								
		HTC Desire 626	LG K7	ZTE 970	Samsung S2	HTC One XL*	Samsung S4*	HTC One Mini*	HTC Desire S*	Moto-E
	Pinterest	NA	As Expected	As Expected	NA	NA	As Expected	As Expected	NA	NA
	SnapChat	NA	As Expected	As Expected	NA	NA	As Expected	As Expected	NA	NA
	WhatsApp	NA	As Expected	As Expected	NA	NA	NA	As Expected	NA	NA
Internet Data	Bookmarks	As Expected	Not As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	History	As Expected	Not As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
	Email	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
GPS Data	Coordinates/Geo-tagged	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Non-Latin Character	Reported in native format	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Hashing	Case File/Individual Files	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected
Case File Data Protection	Modify Case Data	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected	As Expected

**Table 3: Chip-Off Data Extractions**

## 4.2 JTAG Data Extractions

The internal memory contents for JTAG binary images were decoded and analyzed with Forensic Detective v13.1.0.43.

All test cases pertaining to the acquisition of supported Android devices were successful with the exception of the following.

- Facebook social media data was partially reported (i.e., account information) for the HTC One XL.

### Notes:

*-Devices defined in the table below with an '\*' e.g., HTC One Mini\*, both Chip-Off and JTAG data extractions were performed.*

- Deleted Contacts and Calendar entries were recovered for the HTC Desire S and HTC One XL.
- Deleted Contacts were recovered for the HTC One Mini.
- Deleted Contacts, Calendar and Memo/Note entries were recovered for the HTC Samsung S4.
- Deleted Call logs were recovered for the HTC Desire S, HTC One Mini and Samsung S4.
- Deleted SMS entries were recovered for the HTC Desire S, HTC One Mini, HTC One XL and Samsung S4.
- Deleted bookmark entries were recovered for the HTC Desire S and HTC One XL.

See Table 4 below for more details.

Forensic Detective v13.1.0.43					
Test Cases – JTAG Binary Decoding and Analysis		Mobile Device Binary Images: JTAG			
		HTC Desire S*	HTC One Mini*	HTC One XL*	Samsung S4*
Equipment/ User Data	IMEI	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	MEID/ESN	NA	NA	NA	NA
	MSISDN	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
PIM Data	Contacts	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Calendar	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Memos/Notes	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Call Logs	Incoming	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Outgoing	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Missed	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
SMS Messages	Incoming	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Outgoing	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
MMS Messages	Graphic	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Audio	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Video	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Stand-alone Files	Graphic	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Audio	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Video	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Application Data	Documents (txt, pdf files)	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
Social Media Data	Facebook	As <i>Expected</i>	As <i>Expected</i>	Partial	As <i>Expected</i>
	Twitter	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	LinkedIn	NA	NA	NA	NA
	Instagram	NA	As <i>Expected</i>	NA	As <i>Expected</i>

<b>Forensic Detective v13.1.0.43</b>					
<b>Test Cases – JTAG Binary Decoding and Analysis</b>		<i>Mobile Device Binary Images: JTAG</i>			
		<b>HTC Desire S*</b>	<b>HTC One Mini*</b>	<b>HTC One XL*</b>	<b>Samsung S4*</b>
	Pinterest	NA	As <i>Expected</i>	NA	As <i>Expected</i>
	SnapChat	NA	As <i>Expected</i>	NA	As <i>Expected</i>
	WhatsApp	NA	As <i>Expected</i>	NA	NA
<b>Internet Data</b>	Bookmarks	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	History	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
	Email	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
<b>GPS Data</b>	Coordinates/ Geo-tagged	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
<b>Non-Latin Character</b>	Reported in native format	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
<b>Hashing</b>	Case File/ Individual Files	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>
<b>Case File Data Protection</b>	Modify Case Data	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>	As <i>Expected</i>

**Table 4: JTAG Data Extractions**